



| Brief |

Introduction to Social Engineering: Business Email Compromise

B-2024-04-11a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Social Engineering, Phishing, BEC

April 11, 2024

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were *identified prior to 9:00 AM (EDT) on April 11, 2024*; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief | Introduction to Social Engineering: Business Email Compromise

ZeroFox's Social Engineering series breaks down aspects of the threat into digestible reports and outlines defensive actions that can be taken to combat it. Part Five of this series takes a deep dive into Business Email Compromise (BEC), why and how threat actors do it, and how the threat can best be mitigated.

Key Points

- BEC is a high-effort phishing technique in which a threat actor targets the legitimate email addresses of organizations and individuals, tricking users into providing sensitive information which can lead to monetary theft or enable further malicious activity.
- Reporting suggests that BEC attacks are on a sharp upward trajectory, which is very likely due in part to their relatively high success rates and payoff in comparison to other methods of cyberattack.
- BEC is almost certain to remain a pertinent threat to organizations across industries in 2024, as threat actors continue to capitalize upon established techniques, high success rates, and constantly increasing financial payoffs.

| What is Business Email Compromise?

BEC is a high-effort phishing technique in which a threat actor targets the legitimate email addresses of organizations and individuals, tricking users into providing sensitive information which can lead to monetary theft or enable further malicious activity. These attacks often leverage a multitude of other cyber threat vectors to obtain the information necessary to conduct highly targeted pretexting and spear phishing activity and are usually heavily reliant upon social engineering techniques that allow innate human curiosities to be exploited. BEC attacks are also often enhanced by the leveraging of personal and organizational information gained from previous cyberattacks.

According to reporting from the Federal Bureau of Investigation (FBI), BEC incurred the second-highest average cost for victim organizations amongst all types of cyberattacks during 2023.¹ This cost has reportedly increased significantly over the past five years to an approximate median of USD 50,000 and remains on a steep upward trajectory.² Although entities of all sizes are at risk of being victimized by BEC attacks, larger organizations very likely have the highest probability of being targeted. This is due, in part, to large organizations' higher number of potential threat vectors, often fragmented communications, and reporting procedures unclear to employees.

The specific techniques used in BEC attacks vary, but most leverage a variety of the stages described below.

Reconnaissance. The attacker seeks an organization deemed to be a potentially lucrative, high-payoff target. Both illicit and licit research methods are used, including:

- Open source internet research leveraging publicly available websites, media articles, and press releases.
- Harvesting of organizational email addresses from public websites, forums, and social media platforms. Various web scraping tools, crawlers, and domain name system (DNS) enumeration techniques can be used to enhance this process.

¹ [hXXps://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf](https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf)

² [hXXps://www.verizon.com/business/resources/T9a1/reports/2023-data-breach-investigations-report-dbir.pdf](https://www.verizon.com/business/resources/T9a1/reports/2023-data-breach-investigations-report-dbir.pdf)

- Monitoring of deep and dark web (DDW) forums, whereby a threat actor may be able to obtain credentials or other sensitive information leaked during previous malicious activity.
- Social engineering, whereby a threat actor poses as an external entity such as a supplier, customer, or IT services provider. The employees most likely to be approached are those in frequent contact with external third parties, those able to access sensitive personal information, and newer employees that are unfamiliar with organizational IT protocol.

The feasibility of a potential victim organization often depends heavily on the extent of information that can be determined about it in advance of attack, as this significantly enhances the threat actor's ability to conduct targeted social engineering activity. Information considered valuable includes that surrounding organizational hierarchies and reporting chains, the names and positions of stakeholders, communication methods and behaviors, and insight into supply chain relationships.

Target Selection. Upon choosing an organization, the threat actor conducts further research into their employees and practices, seeking both an opportunity that can be exploited and the employees whose successful targeting is most likely to enable it. To achieve this, phishing attacks can be leveraged to establish information that is not publicly available, such as details surrounding relationships with third parties, pending transactions, company events, and cybersecurity protocols.

It is likely that newer, more junior employees are at the highest risk of phishing attacks seeking to obtain this information due to perceived lower vigilance against social engineering attacks, unfamiliarity with organizational security protocols, and the higher chance that punitive repercussions will deter them from reporting activity deemed suspicious.

Business Email Compromise. Once an exploitable opportunity is identified, the threat actor seeks to intercept associated communications by masquerading as a legitimate employee. There are a number of different ways that this can be achieved, though they can be separated into two broad categories: spoofing and account takeover.

- *Spoofing.* In order to convincingly impersonate an employee, threat actors spoof several aspects of email communications, making them appear legitimate. The extent of spoofing deployed is dependent on the security protocols implemented by the victim organization, as well as the attacker's technical expertise and expected payoff.
 - *Address Spoofing.* The threat actor creates a new email address designed to imitate that of an employee. The username, mail server, subdomain, or the top-level domain (TLD) can be spoofed, usually by adding, omitting, or replacing characters with the intent that the discrepancy goes unnoticed.

Correct email address: socialengineering@example.spooxing.com

Spoofed username: s0cialengineering@example.spooxing.com

Spoofed subdomain: socialengineering@exanmple.spooxing.com

Spoofed domain: socialengineering@example.sp0ofing.com

Spoofed TLD: socialengineering@example.spooxing.net

This technique requires minimal technical expertise and can be deployed readily by threat actors leveraging free or low-cost domains. However, many email platforms have the capability to detect this activity, resulting in the user being notified, and the email address or the sender being condemned.

- *Display Name Spoofing.* An email address is created and registered using the same name as the individual being impersonated. Many email platforms display the sender's username rather than the full email address or any other metadata—particularly mobile apps, which are becoming more prevalent.

Additionally, threat actors often use a believable email address as a display name so that victims see what appears to be a legitimate email address in the header of the message. While display name spoofing is

simple to implement when using certain email platforms, this type of spoofing can be easy to identify due to the inability to alter the associated email address.

- *Email Spoofing.* This primarily refers to the manipulation of the “From” field, allowing an email to appear as though it has been sent by a different email address than the one displayed. Malicious actors can achieve this by exploiting vulnerabilities found in misconfigured Simple Mail Transfer Protocol (SMTP) servers or by leveraging certain phishing kits. This technique can enable the threat actor to circumvent some authentication protocols but requires more technical expertise than address and display name spoofing.
- *Content.* The attacker uses social engineering techniques such as familiarity, relevance, urgency, direction, and fabricated implications to increase the likelihood of victim interaction. Correctly populated, timed, and appropriated, this will increase the likelihood of the victim overlooking discrepancies in other aspects of the email.
- *Account Takeover.* Also referred to as Email Account Compromise (EAC), these higher-effort, complex attacks involve the threat actor gaining illicit access to a target employee’s email account. This offers the attacker unhindered access to contacts, correspondence, and personal identifiable information (PII), as well as the ability to send legitimate communications to colleagues and third parties without scrutinization from either the email servers or the message recipients.

There are several methods a threat actor can leverage to obtain control of a legitimate mailbox. Login credentials may have been procured through malicious marketplaces, or the victim may have already been subject to a successful phishing attack in which the information was unintentionally disclosed. There is also a smaller chance that the account was compromised through password guessing attacks, such as brute force or credential stuffing.

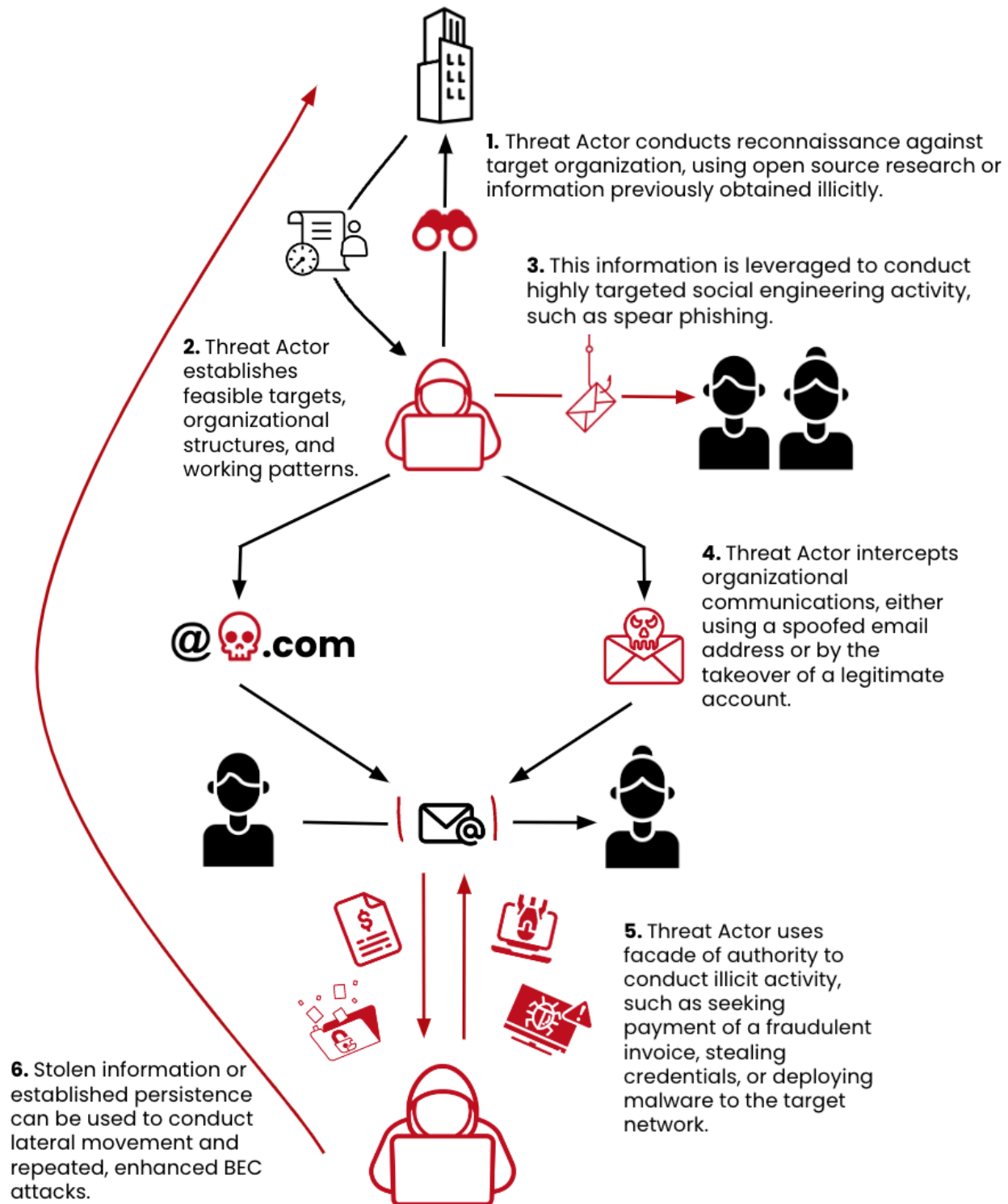
This access enables the threat actor to conduct further malicious activity, such as extortion, malware deployment, data theft, or credential harvesting. Espionage and sabotage could also take place, though this is more likely if the attacker is politically or ideologically-motivated and seeking to obtain proprietary or sensitive information or cause organizational disruption.

Evasion, Persistence, and Exit. It is very likely that the majority of BEC attacks are planned and conducted with the aim of compromising an anticipated action or circumstance. In such a case, the threat actor likely assumes that any malicious presence would be revealed following a successful attack (for example, the interception of a payment between an organization and a supplier). Exit is likely the threat actor's next priority in order to maintain a low profile and minimize subsequent law enforcement scrutiny.

In some cases, threat actors establish quiet persistence, using any illicit access acquired to conduct further, in-depth reconnaissance and research activities. This can enable a future, highly targeted cyberattack with the extensive pre-planning offering a heightened chance of success. During this time period, the attacker is very likely to restrain from conducting activity that may alert the victim to their presence, such as adjusting mailbox settings, changing credentials, or using the email address to conduct overt attacks. The threat actor can also deploy malware to the target network, enabling further persistence, lateral movement, or the theft of information via stealers or spyware.

BEC attacks are usually conducted by financially motivated threat actors seeking to steal funds, but other actors such as nation-state affiliates or business competitors also have an interest in causing organizational disruption or stealing proprietary information. Reporting suggests that the frequency of BEC attacks is on a sharp upward trajectory, which is very likely due in part to their relatively high success rate and payoff in comparison to other cyberattack methods.³

³ [hXXps://abnormalsecurity\[.\]com/blog/bec-vec-attacks](https://abnormalsecurity.com/blog/bec-vec-attacks)



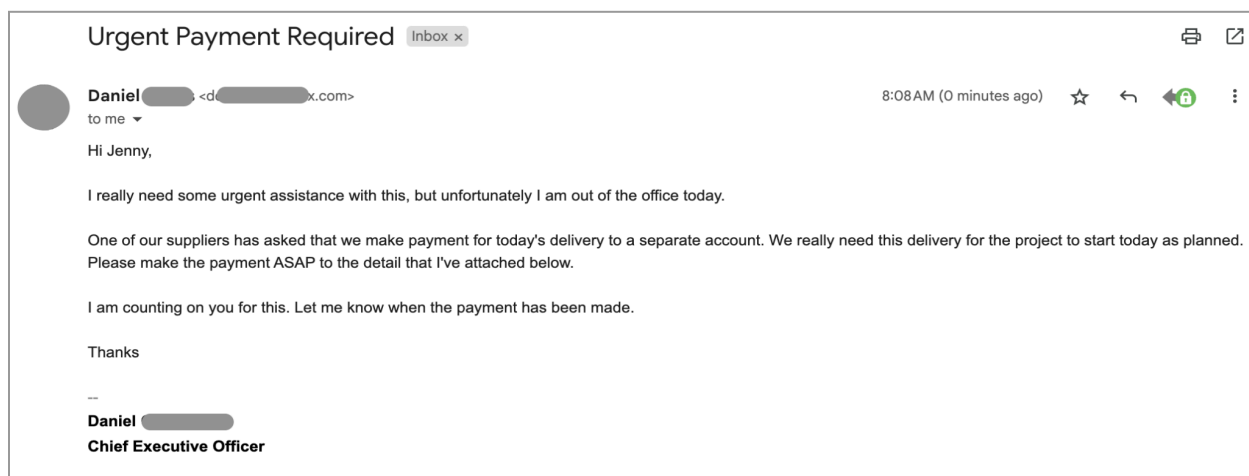
High-level overview of how a BEC attack could take place

Source: ZeroFox Intelligence

| Business Email Compromise Methods

By conducting sufficient research and establishing an impersonation method, threat actors can implement themselves into a multitude of different situations that are vulnerable to exploitation. The nature of these evolves over time and varies across industries, as threat actors continually seek to exploit contemporary vulnerabilities and leverage topical lures. However, these are some of the professional interactions and situations most prominently leveraged in BEC attacks.

Executive Impersonation. Also known as CEO Fraud or Whaling, the attacker poses as a company executive or other key stakeholder in order to use their implicit authority to make illegitimate demands of employees. Upon establishing a spoofed method of communication, the attacker demands a sum of money or sensitive information. Various social engineering techniques are also employed to enhance the chances of success, such as implying a sense of urgency, responsibility, and possible implications for failure to comply.



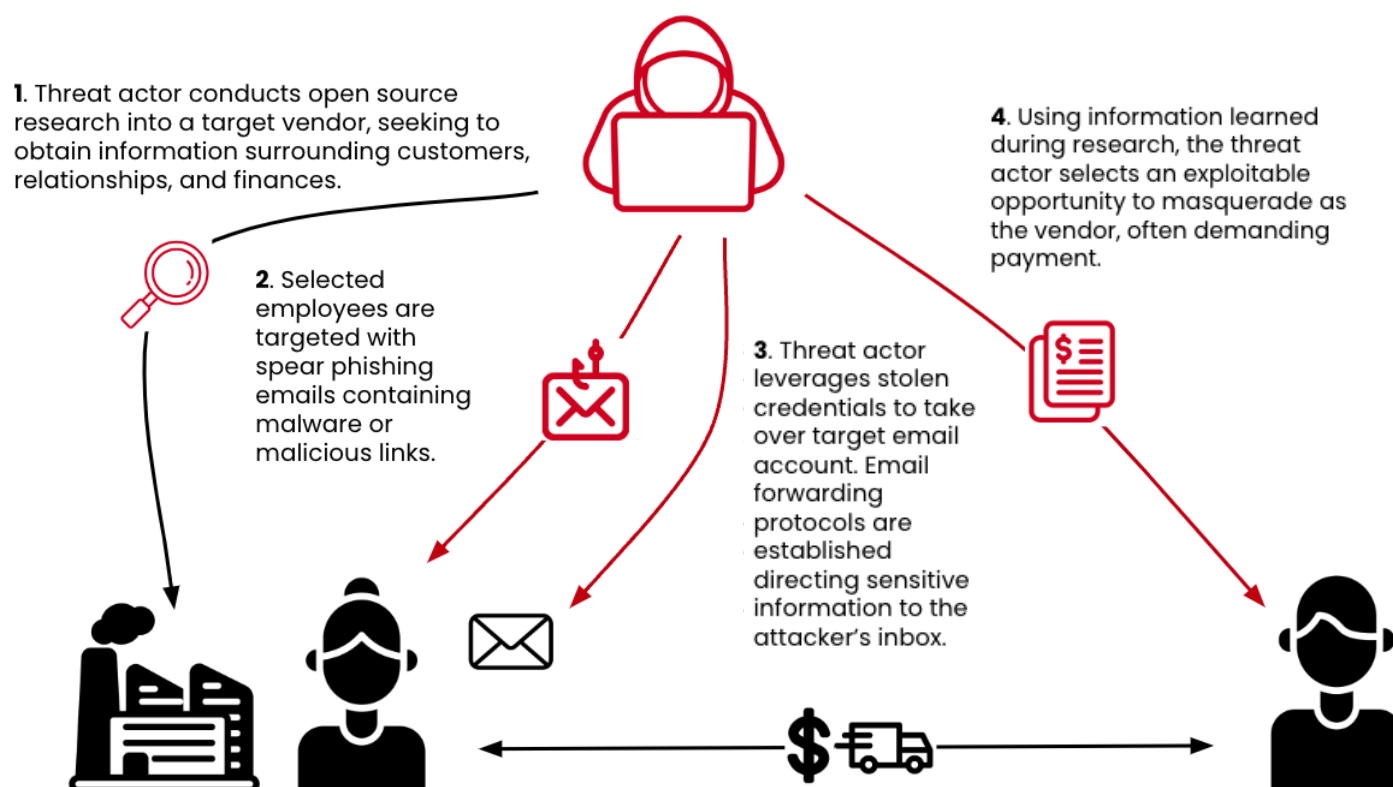
Example of how an Executive Impersonation attack could take place

Source: ZeroFox Intelligence

Executive Impersonation is very likely deemed by threat actors as one of the most lucrative BEC attack methods that can be conducted, due to the flexibility offered by the perceived authority of a senior figure and the ease of researching their often-public profile. Reporting suggests that, of the approximately 80 percent of organizations that

were targeted by fraudulent attacks in 2023, almost half were victims of Executive Impersonation. The most dreaded impacts organizations reported were damaged supplier relationships and a tarnished reputation with investors and customers.⁴ When successful, these attacks can also lead to significant financial damage, the firing of staff, and legal scrutiny.

Vendor Email Compromise (VEC). During BEC attacks, the threat actor impersonates an associated vendor, supplier, or other associate. These attacks very likely require extensive research into the standard operating procedures of both organizations, their business transactions, and the personal relationships that may be exploited. To achieve this level of reconnaissance, threat actors compromise email accounts via phishing methods, before creating email forwarding rules that direct the messages to the attacker's inbox.



Example of how a VEC attack could take place

Source: ZeroFox Intelligence

⁴ [hXXps://5278241.fs1.hubspotusercontent-na1\[.\]net](https://5278241.fs1.hubspotusercontent-na1[.]net)

While this alone would almost certainly provide access to financial information that could be implicated in a revenue-generating attack, a successful VEC often waits until a pertinent moment to demand an illicit payment. This is also known as a False Invoice Scam.

This attack method benefits the threat actor; by masquerading as an external party, the victim is less likely to discern suspicious behavior or that which is inconsistent with their usually expected standards. VEC attacks are very likely to become more common as supply chains become increasingly complex and opaque, leading to challenges in understanding the standards adhered to by supply chains. The frequency of these attacks are reported to have increased by 50 percent consecutively during 2022 and 2023, with the construction, retail, and automotive industries the most targeted.⁵

Attorney Impersonation. In these attacks, threat actors pose as a representative of a firm offering legal services, masquerading as an attorney or solicitor. Feasible targets include providers of industry-specific legislative support, equality advisory and support services (EASS), health and safety advisors, or firms involved in any ongoing legal proceedings.

Research is first conducted into the target organization, leveraging phishing techniques and email account takeover to obtain details surrounding its relationships with legal services providers. The attack is then planned in accordance with the desired ends, which may be the acquisition of funds in return for previously undertaken or to-be-provided services, theft of PII (including the personal details of employees), or the theft of proprietary information regarding the organization's ongoing projects, output, partnerships, or research.

Threat actors conducting attorney impersonation attacks are less likely to target senior employees or key stakeholders due to the elevated risk of arousing suspicion. Instead, newer employees or those not adept in legal correspondence are targeted leveraging social engineering techniques to encourage a response, including techniques such as an urge for secrecy. Spoofed web pages that mimic a law firm may also be deployed that are equipped with malicious software designed to steal credentials.

⁵ [hXXps://abnormalsecurity\[.\]com/blog/vec-attacks](https://abnormalsecurity.com/blog/vec-attacks)

| Case Study

ZeroFox recently investigated a case involving a media and entertainment company whereby a threat actor attempted to carry out unauthorized updates to direct deposit information. The threat actor leveraged multiple look-a-like domains as part of a series of phishing messages to socially engineer users into providing credentials and multi-factor authentication (MFA) codes. In parallel, the threat actor performed a Search Engine Optimization (SEO) poisoning campaign using Google Ads to direct users to additional malicious login sites. Multiple users fell victim to the phishing scheme, and their access to the employee portal was leveraged to request changes to direct deposit information.

There was a weakness in the direct deposit change process on the company's side whereby a user was informed a change had been made to their direct deposit versus validation through a secondary trusted method being required for authentication.

ZeroFox assisted by helping to investigate the unauthorized updates along with enhanced domain monitoring and takedown services on the malicious domains. ZeroFox recommended enhancements to the company's direct deposit validation process by requiring user approval through a trusted method before processing changes, along with having a web beacon installed on corporate login sites to improve the detection of cloned pages.

Resilience – Business Email Compromise

- *Organizations should implement training for employees focusing on awareness of contemporary threats, phishing vigilance, social engineering resilience, and basic cybersecurity hygiene.*
- *Help to protect against the spoofing of corporate email domains and servers by implementing a secure email gateway (SEG) and authentication protocols such as Sender Policy Framework (SPF); DomainKeys Identified Mail (DKIM); and Domain-based Message Authentication, Reporting, and Conformance (DMARC).*
- *Ensure employees are aware of the potential implications of a large online footprint and how their personal information can be used to target them with spear phishing and BEC attacks.*
- *Employees should be aware of the steps to take if they suspect their email account has been compromised. Initial steps include resetting of passwords, removing unknown email forwarding rules, and checking if the address has been blocked from sending mail in response to its association with suspicious activity. Further instructions can be found at:*
 - *[hXXps://learn.microsoft\[.\]com/en-us/microsoft-365/security/office-365-security/responding-to-a-compromised-email-account?view=o365-worldwide](https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/responding-to-a-compromised-email-account?view=o365-worldwide)*
- *Any changes made to employee personal information or direct deposit details via an external platform should require secondary authorization by a trusted figure.*
- *If an email seems suspicious, scrutinize the full email header. This contains information from all email components, such as the From, To, Date, and Subject fields. Metadata will also reveal the routing history, original location, and the status of reporting protocols.*
- *As the most secure form of MFA, physical authentication devices should be used where possible. Devices such as USB and public key infrastructure (PKI) keys are the least susceptible to interception, tampering, or compromise.*

| Outlook

BEC is almost certain to remain a high threat to organizations across industries in 2024, as threat actors continue to capitalize upon established techniques, high success rates, and constantly increasing financial payoffs. While executive impersonation, BEC, and VEC will almost certainly persist, it is very likely that new techniques will emerge exploiting topical lures and contemporary security culture.

As organizations and their employees become more adept at identifying and mitigating lower-effort social engineering attacks, threat actors are very likely to increasingly opt for bespoke, highly targeted attacks such as BEC, which—while still reliant upon the vulnerable human aspect of a network—can apply the research and tools needed to heighten the chances of success. Threat actors are likely to continue prioritizing the targeting of larger organizations due to higher potential vulnerabilities to be exploited, as well as a perception of higher payoffs should the attack be successful. Smaller organizations will also be targeted by BEC attacks, though threat actors are more likely to leverage lower-effort techniques such as address spoofing.

Threat actors are almost certain to capitalize upon the growing online footprint of organizations and individuals, leveraging social media platforms, online forums, and publicly available information to conduct the research necessary to support future attacks. The increasing complexity and dispersion of organizational partnerships, the consumer base, and supply chains are very likely to further exacerbate this by introducing further potentially vulnerable threat vectors and obfuscating the expected and adhered to standards of cybersecurity.

| Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%